DRegard@lecg.com
12/13/2004 03:36 PM

To Peter_McCabe@ao.uscourts.gov
cc
Subject Request to Testify in Dallas

04-CV-044
Request To Testify
1/28 Dallas

December 13, 2004

Dear Mr. McCabe:

This e-mail will serve as my formal request to testify on proposed e-discovery rules in Dallas, Texas on January 28 , 2005.
I appreciate the opportunity to be part of this process.
If you require additional information from me regarding the above, please contact me via e-mail.

Thank you,

Dan Regard, Esq.
Managing Director
LECG, LLC

t: +1.202.973.6481
c: +1.202.550.4764
dregard@lecg.com

January 20, 2005

04-CV-044
Testimony
1/28 Dallas

Mr. Peter G. McCabe, Secretary
Committee on Rules of Practice and Procedure
Administrative Office of the United States Courts
Thurgood Marshall Federal Judicial Building
Washington, D.C. 20544

Re: Proposed E-Discovery Amendments to Federal Rules of Civil Procedure

Dear Mr. McCabe:

I am scheduled to testify at the January 28, 2005 hearing in Dallas. I anticipate my testimony will encompass the talking points attached.

I thank you for your attention and look forward to testifying in Dallas.

Respectfully submitted,

Daniel Regard

Cc: John Rabiej, Chief of Staff
Judy Krivits

Testimony Outline for Dan Regard

Introductory Remarks

1. I am Daniel Regard, a Managing Director in the Washington DC office of LECG. LECG is a global expert services firm that offers expert testimony, original research and consulting. My area of specialization is electronic discovery. I have been a consultant in the computer industry for more than 20 years. I hold a B.S. in Computer Science, a JD and an MBA. I have come to testify today because I believe I bring a unique perspective to the discussion about the proposed amendments to the Federal Rules of Civil Procedure.

2. This perspective has evolved from my direct experience with the technologies that have created the situation before us. I believe there is a commonly held assumption that technology has gotten us into this muddle — and technology should, or can get us out of it. I believe this is misguided.

3. Today, I would like to make some general comments about the technologies that have inspired this quest for a better way to deal with electronic discovery, and offer my opinion on three of the proposed amendments.

Technology

1. Technology poses unique, exciting and formidable challenges. It has made the process of discovery in litigation complex and costly. This is not the "fault" of any specific party — it a natural consequence of the disconnect between the pace of technological change and the inability of business processes to keep up with it.

2. Insofar as the use of technology to solve the problems it has created, it is inadequate and imperfect. What it has done is shift the burden. Whereas technology may allow for larger volumes to be *copied* and *transferred* easily, the searching capability afforded by technology is elusive. This is where burdens are unequal. The ability to search thousands, or millions of files helps where you are looking for a single document. But if you are *producing* information in a discovery, you cannot stop after you've found one privileged document. You need to find and mark them all. That is the difference: the difference between *one* and *all*. Search technology helps much more with finding the *one* than with finding the *all*.

Reasonably Accessible

1. While the intention of this amendment is good, I am opposed to it.

"Reasonably Accessible" Electronic Information (Rule 26(b)(2)).

Rule 26(b)(2) would be amended to permit a party to object to a discovery request that calls for electronically stored information that is not "reasonably accessible," requiring a motion to compel to obtain the data:

A party need not provide discovery of electronically stored information that the party identifies as not reasonably accessible. On motion by the requesting party, the responding party must show that the information is not reasonably accessible. If that showing is made, the court may order discovery of the information for good cause and may specify terms and conditions for such discovery.

2. The term "reasonably accessible" may soon be (or already is) outdated. The phrase has mostly been used in the sense of "online" versus "offline." Data that is live and accessible, versus data that is stored offline and may be difficult to access due to age, manner, technological changes, etc.

3. Data stored off-line may be becoming a disappearing concept and practice. Corporations are actively considering or implementing "hot-sites" that rely on duplicate live systems rather than backup systems for recovery. Backup tapes are being used in those organizations for short-term (e.g., one week or less) storage. As another example, Google has recently released their online email system, gmail. With gmail you are encouraged "don't throw anything away" (see www.gmail.google.com). Under such a scenario, literally everything is "reasonably accessible."

4. Finally, the aspect of burden seems to be well covered in 26(b)(2)(iii)

Claw Back

1. I am in favor of this amendment. One reason is the unprecedented volumes that parties must contend with. The second is because of the varying degrees of difficulty presented in locating and reviewing different types of information in the production of electronic data.

Claw-Back of Privileged Information (Rule 26(b)(5)).
The proposed amendment to Rule 26(b)(5) would renumber the existing provision Rule 26(b)(5)(A) (Privileged Information Withheld), and add a new Rule 26(b)(5)(B):

Privileged information produced. When a party produces information without intending to waive a claim of privilege it may, within a reasonable time, notify any party that received the information of its claim of privilege. After being notified, a party must promptly return, sequester or destroy the specified information and any copies. The producing party must comply with Rule 26(b)(5)(A) with regard to the information and preserve it pending a ruling by the court.

2. I am in favor of providing parties the ability to assert privilege over produced information. Because of the volumes, the review for privilege is fast becoming a strained process. The ability for a small group of highly knowledgeable individuals to review a production is gone in many of our larger cases. Instead, manpower has been deployed to look for various types of privilege, all under a default rule-imposed time frame.

3. The pressure to handle the increasing volumes must have a safety-release valve. This amendment can provide that valve.

4. Further consideration should also be given to the fact that some electronic information may be easily discernable (e.g., the contents of an email) while other information may be only with great difficulty or using specialized tools. Not all types of imbedded information in various spreadsheet and document files are documented. Hence, the ability to find and review data, which may be privileged or the basis for a privilege, may not be equal among parties. As such, only with greater difficulty might some parties actually become later aware of the full extent of information in their own files. For this reason, as well, I am in favor of a rule providing parties the ability to assert privilege over produced information.

Safe Harbor

1. I am in favor of a Safe Harbor from sanctions.

Sanctions Safe Harbor (Rule 37(f)).
A new Rule 37(f) includes a safe harbor from sanctions relating exclusively to electronically stored information:

Electronically Stored Information. Unless a party violated an order in the action requiring it to preserve electronically stored information, a court may not impose sanctions under these rules on the party for failing to provide such information if:

a. the party took reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action; and

b. the failure resulted from loss of the information because of the routine operation of the party's electronic information system.

2. I have been in a number of preservation situations. Some have been easy, some complex. Based on my experience, I would caution the Committee to look beyond the relatively well- understood paradigm of emails and user files to consider the more complex environment of database systems.

3. Large database systems such as Oracle, JD Edwards, PeopleSoft and many other custom systems are different from email systems. Identifying all the various areas

within a complex system that are responsive takes a significant investment of time and effort. While this process is taking place, automated processes often are deleting information. And the ability for companies to turn off deletion processes can be limited, at best, impossible at worst.

4. Large systems, while capable of being copied (sometimes) as a single "snapshot," may be limit restoration of that snapshot only on the system from which it was copied.

5. There may be data in the system, temporary or transactional tables, that were never created or intended to be retained for any measurable duration of time. Changing these schedules may be difficult, and the ability to store the resulting data streams may be impossible.

6. As an example, consider an energy company that tracks 19,000 data points per second. This information is then summarized and discarded. Were it necessary to keep the data for any duration, significant amounts — gigabytes and terabytes — of storage would be required.

7. With time to act reasonably, trained engineers, data users and litigation experts can examine the system. A targeted capture can be made. Data can be preserved as appropriate.